REMARKS

The objections to the claims should be withdrawn in view of the Amendment to claim 18 and redesignation of claims 16 and 18.

Claims 1-3 were rejected under 35 U.S.C. §102(b) as being anticipated by Holloway et al. (US 5,805,801) in view of Sofer et al. (US 5,489,896). The applicant respectfully traverses this rejection for the following reason(s).

We will assume the rejection is under §103(a) and rejects all claims.

Claim 1

Claim 1 calls for, in part, *detecting, in an address table, access vectors corresponding to the MAC destination and source addresses.*

The combination of applied art fails to teach the foregoing feature.

Holloway's invention relates to systems and methods for detecting and preventing intrusion into a campus local area network by an unauthorized user. A managed hub discovers each interconnect device in the network that supports the security feature and maintains an interconnect device list of such devices, which may include token ring switches, Ethernet switches, bridges and routers. The managed hub determines the interconnect devices in the campus network that are capable of supporting a local area network (LAN) security feature. The managed hub then uses the responses to build and maintain a table of interconnect devices in the network that support the

security feature. Here, during a discovery phase, the managed hub periodically sends a discovery frame to a LAN security feature group address. The managed hub detects an intrusion by an unauthorized address on one of its ports by comparing the MAC addresses on each port against a list of authorized MAC addresses, disables the port and notifies the other interconnect devices in the network of the intrusion by transmitting a security breach detected frame to the LAN security feature group address. The interconnect devices set a filter on their respective ports against the intruding unauthorized address.

Sofer's invention relates to a security unit for a network having a data bus to which a plurality of stations (interconnect devices) can be connected wherein the security unit monitors traffic on the data bus and only enables authorized data to flow along the data bus. The data bus and the security unit are part of a hub. The traffic includes a multiplicity of data packets each having source and destination addresses and the security unit includes a plurality of correlators for determining that the source and destination addresses indicate an authorized communication. Additionally, each station is connected to the data bus via a port having a port address and one of the correlators correlates the source address with an authorized port address.

Note that Sofer's port address is not the same nor equivalent to a destination address, as Sofer clearly differentiates the two addresses. A destination address is the final destination for the message, where the port address is for a particular port connected to the final destination.

Sofer differs from Holloway in that Sofer teaches the destination station address be in a list of authorized destination station addresses for the source station address, because Sofer is concerned with permitting two stations being authorized to communicate with each other. Holloway is only

-12-

concerned with intrusion by an unauthorized source station outside the network breaking into the network via one of the ports. There is no concern with whether a source station is authorized to connect to a destination station.

If one of ordinary skill in the art were motivated to modify the security of a network utilizing Holloway's system in the manner taught by Sofer, then the skilled artisan would modify the system as taught by Sofer.

Here, Sofer discloses an authorization unit 44 that comprises three correlators 50, 52 and 54, a mode switch 56 and a decision unit 58. Correlator 50 determines whether or not the source station address is among authorized source stations. Correlator 52 determines whether or not the source station address is attached to its corresponding port, where the port address is provided from a hub 20, in the case of the LET 36 hub. Correlator 54 determines whether or not the source station is allowed to communicate with the destination station. Each of correlators 50-54 comprise a list of authorized relationships. Thus, correlator 50 has a list of authorized stations, correlator 52 has a list of source addresses and their corresponding port addresses and correlator 54 has a list of source addresses and their allowed destination addresses.

As mentioned above, claim 1 calls for *detecting, in an address table, access vectors corresponding to the MAC destination and source addresses.*

None of Sofer's correlators utilize access vectors, but instead use specific addresses, and similarly Holloway discloses the use of an authorized address list (AAL) controls which MAC addresses are allowed to connect to <u>specified ports</u>. Each entry in the AAL consists of two fields: port number and authorized address. The port number identifies a specific port on the hub; the

-13-

authorized address field specifies the address or addresses that are allowed to connect to the port. The AAL (Authorized Address List) defines which MAC source addresses, *i.e.,* authorized source address, are allowed to connect to specific ports on the hub.

Accordingly, neither of the applied references would have taught one of ordinary skill in the art to utilize *access vectors*, which are not equivalent to access addresses, instead of MAC addresses.

The present invention has an advantage over the applied art, because of its use of access vectors. An access vector consists of a bit vector. The bit value "0" means restriction to access and "1" means allowance for access. For example, if a server node S1 has an access vector 00010000 and a client node C1 has access vector 10000001, then client node (source station) C1 cannot access server node (destination station) S1, but another client node C2 having access vector 00010001 can access server node S1.

For further understanding, access vector 00010000 of a server node S1 means that S1's HostID is 3, and its access vector is 0x80>>3. If C1 is going to be an access client node, the access vector of C1 should be (0x80>>3). If the access vector of C1 is 10010001, then this access vector 10010001 means C1 can access server nodes that have HostID 0, 3 or 7. Thus a client node having an access vector xxx1xxxx (x can be a 0 or 1) can access a server node having a HostID of 3, and a client node having an access vector xxx0xxxx (x can be a 0 or 1) is restricted from accessing a server node having a HostID of 3.

Accordingly, it is possible to use the same (e.g., 8-bit) access vectors for more than one (32-bit) source address and (32-bit) destination address, thereby saving memory space for storing the correlating 8-bit access vectors instead of correlating each 32-bit source address and destination

-14-

address.

Therefore, since the present invention utilizes access vectors instead of the MAC addresses of the prior art, and the applied art fails to teach or move one of ordinary skill in the art to use anything other than MAC addresses for preventing or allowing access, the rejection of claim 1 is deemed to be in error and should be withdrawn.

Claim 19 is nonobvious for the same reasons as claim 1 .

Claim 2

With respect to claim 2, Sofer was not applied against any of the specific features of claim 2.

Claim 2 calls for *configuring an anti-hacker table comprising information pertaining to a plurality of client nodes and a plurality of server nodes of a network, wherein each client node is identified by a corresponding MAC address, a corresponding host identification and a corresponding IP (Internet protocol) address, and each server node is identified by a corresponding MAC address, a corresponding host identification and a corresponding IP (Internet protocol) address.*

Holloway discloses an anti-hacker table. This table is known as the Authorized Address List (AAL). The Examiner refers to both of Holloway's AAL table and a "Breach list table". The breach list is not part of the AAL table, but instead is an entirely different table used for other purposes that those of the AAL table.

The Examiner acknowledges that Holloway's AAL table and Breach list table do not use an

IP address. Here the examiner refers us to Holloway's disclosure in col. 17, lines 15-17 with respect to an IP address.

Accordingly, Holloway's AAL may comprise a port number, a source MAC address and a source IP address. The AAL does not comprise *a corresponding host identification* address. Additionally, the combination of Sofer and Holloway's AAL would **not** comprise a plurality of server nodes of a network, wherein *each server node is identified by a corresponding host identification.*

Holloway's Breach list table, Fig. 7, includes a source MAC address that was detected as an intruder, the module and <u>port</u> number where the intrusion was detected, the time (sysUpTime) when the security breach was detected, and the outstanding filter set count which is set to the number of entries in the ICD list.. The Breach List contains information on intrusions recognized by the hub and in the process of being secured.

Accordingly, the Breach list table does not comprise *information pertaining to a plurality of client nodes, wherein each client node is identified by a corresponding MAC address, a corresponding host identification and a corresponding IP (Internet protocol)* address. Additionally Holloway's Breach list table does not comprise a plurality of server nodes of a network, wherein *each server node is identified by a corresponding MAC address, a corresponding host identification and a corresponding IP (Internet protocol) address.* In fact there is no need for server node information since the list is for recording information on intruding client (source) stations. Sofer, not applied in this regard, does not provide any teaching suggesting recording server node (destination stations) in Holloway's Breach list table.

-16-

Accordingly, claim 2 is not obvious in view of the applied art, thus the rejection should be withdrawn.

Further, with respect to the step of *determining whether the received MAC source address is stored in said address table* set forth in claim 2, the Examiner refers us to Holloway's step 132

Step 132 in Holloway's Fig. 11, is directed towards discovering what devices are connected to a managed hub in order to create an Interconnect Device List (ICD) which identifies those devices authorized to be connected to the hub.

The Interconnect Device List (ICD) is not part of Holloway's AAL (deemed by the Examiner to be the *access table* set forth in claim 1). Therefore, the feature of *determining whether the received MAC source address is stored in said address table* is not met by Holloway's step 132.

Second, Holloway teaches creating a new Interconnect Device List item using a new source address from the discovery response frame, the device description from the frame, and the time stamp from the frame, and adding it to the Interconnect Device List . Holloway does not disclose storing *the configured address entry for said received MAC source address in said address table when it is determined that said new MAC source address is not stored in said anti-hacker table*. That is, Holloway does not compare the source MAC address in the AAL table based upon a determination of whether or not the source MAC address is stored in an anti-hacker table.

Also, because Holloway does not teach configuring an *address entry for said received MAC*

-17-

source address in said address table, Holloway fails to teach *determining whether said new MAC source address is stored in said anti-hacker table.*

The process depicted in Holloway's Fig. 12 checks all the ports in the hub to ensure that a station attached to the port has been authorized to establish a connection on this port. The AAL (Authorized Address List) defines which MAC addresses are allowed to connect to specific ports on the hub. In step 220 a check is made here to ensure that the address that has been detected on this port is in the list of authorized addresses. If the address detected on the port is authorized, then continue processing at step 230. If the address detected on the port is not in the authorized list, then processing continues at step 250.

Although the address being detected may be a new address not already stored in the AAL table, this is not the same as the new address of Applicant's claim 2. The new MAC address in Holloway is not the result of a step of *configuring an address entry for said received MAC source address when it is determined that said MAC source address is not stored in said address table and identifying said received MAC source address as a new MAC source address.*

Additionally, Holloway's does not teach a process of *storing the configured address entry for said received MAC source address in said address table when it is determined that said new MAC source address is not stored in said anti-hacker table.* Instead Holloway teaches an entry is added to the **Breach List** containing the following: MAC address that was detected as the intruder, the module and port number where the intrusion was detected, the time (sysUpTime) when the security breach was detected, and the outstanding filter set count which is set to the number of entries in the ICD list. As discussed above, Holloway's *address table* has been determined by the Examiner

-18-

to be the AAL table, and as taught by step 265, the new MAC address in the Breach List, however, the Breach List is not a part of the AAL table.

Accordingly, the rejection of claim 2 is deemed to be in error and should be withdrawn. Claim 20 is nonobvious for the same reasons as claim 2.

Claim 3

With respect to claim 3, Sofer was not applied against any of the specific features of claim 3.

Claim 3 calls for *modifying an access vector included in said configured address entry for said new MAC source address, to set security; and*

storing the configured address entry including the modified access vector for said new MAC source address in said address table

The Examiner refers to step 320 of Fig. 13, and steps 320 and 322, respectively.

In step 320, a filter is set for the intruding MAC address on the current port. Processing then continues at step 322. In step 322, a check is made to determine if the filter processing has been applied to all of the ports in the interconnect device.

There is no discussion of access vectors nor in changing any part of Holloway's AAL (deemed by the Examiner to be the *access table* set forth in claim 1).

Accordingly, the rejection of claim 3 is deemed to be in error and should be withdrawn.

Claims 18 and 21 are not obvious for the same reason's as claim 3.

Claim 4

Claim 4 calls for, in part, *address table storing registered MAC addresses, source access vectors corresponding to source MAC addresses of said registered MAC addresses and destination access vectors corresponding to destination MAC addresses of said registered MAC addresses.*

As discussed with respect to claim 1, the combined teachings of Holloway and Sofer fails to suggest using source address vectors and destination access vectors.

Accordingly, claim 4 is deemed to be nonobvious for the same reason as claim 1. Thus the rejection shgould be withdrawn.

Claim 4 also calls for *packet memory storing received data packets, said packet memory including a port table and an address table.*

Here, the Examiner appears to apply only Holloway's teachings in this regard, by referring to Holloway's Col. 3, lines 7-9, and Fig. 9 which is the Interconnect Device List and the corresponding description thereof in Holloway's specification. There is no teaching of a packet memory anywhere in Holloway, much less the cited sections thereof.

Accordingly, claim 4 is deemed to be in error and should be withdrawn.
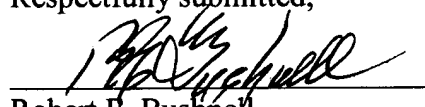
Claims 5-21 are deemed to be nonobvious for the same reasons as claims 1-4 as discussed

above.

The Examiner is respectfully requested to reconsider the application, withdraw the objections and/or rejections and pass the application to issue in view of the above amendments and/or remarks.

No fee is incurred by this Amendment. Should a Petition for extension of time be required with the filing of this Amendment, the Commissioner is kindly requested to treat this paragraph as such a request and is authorized to charge Deposit Account No. 02-4943 of Applicant's undersigned attorney in the amount of the incurred fee if, **and only if**, a petition for extension of time be required **and** a check of the requisite amount is not enclosed.

Respectfully submitted,

Robert E. Bushnell
Attorney for Applicant
Reg. No.: 27,774

1522 K Street, N.W.
Washington, D.C. 20005
(202) 408-9040

Folio: P56339
Date: 9/15/05
I.D.: REB/MDP

-21-